INFORMATION AND COMPUTATION 112, 51–54 (1994)

The BNS Lower Bound for Multi-party Protocols Is Nearly Optimal

VINCE GROLMUSZ

Department of Computer Science, Eötvös Loránd University, 1364 Budapest, Hungary

We present a *multi-party protocol* which computes the *Generalized Inner Product* (GIP) function, introduced by Babai *et al.* (1989, in "Proceedings, 21st ACM STOC," pp. 1–11). Our protocol shows that the lower bound for the multi-party communication complexity of the GIP function, given by Babai *et al.*, cannot be improved significantly. © 1994 Academic Press, Inc.

1. INTRODUCTION

In the two-party communication game, introduced by Yao (1979), there are two players, P_0 and P_1, and a function $f: \{0,1\}^{2n} \to \{0,1\}$. The goal of the players is to compute the value of $f(A_0, A_1)$ cooperatively, for some $A_0, A_1 \in \{0,1\}^n$, where A_0 is known only to P_1, A_1 is known only to P_0, and after the computation both players should know the value $f(A_0, A_1)$. The players have unlimited computational power, and both know the definition of f. P_0 and P_1 communicate via a blackboard, which is seen by both of them: they are allowed to write bits on the blackboard. The cost of the computation is the number of bits communicated. Since the players have unlimited computational power, every function can be computed by communicating $n+1$ bits.

The following generalization of the two-party communication game by Chandra *et al.* (1983) has led to some nice results in complexity theory (cf. Babai *et al.*, 1989: Goldmann and Håstad, 1990): In the multi-party communication game, k players, $P_0, P_1, ..., P_{k-1}$ intend to compute the value of $g(A_0, A_1, ..., A_{k-1})$ cooperatively, where $g: \{0,1\}^{kn} \to \{0,1\}$ and $A_i \in \{0,1\}^n$, for $i = 0, 1, ..., k-1$. Player P_i knows the value of each variable, except A_i, for $i = 0, 1, ..., k-1$. As in the two-party game, the players have unlimited computational power, and they communicate with the help of a blackboard, viewed by all players. Only one player may write on the blackboard at a time. The goal is to compute $g(A_0, A_1, ..., A_{k-1})$, such that at the end of the computation, all players know this value. The cost of the computation is the number of bits written on the backboard for

0890-5401/94 $6.00

the given $A=(A_0, A_1, ..., A_{k-1}) \in \{0,1\}^{nk}$. The cost of a multi-party protocol is the maximum number of bits communicated for any A from $\{0,1\}^{n\times k}$. The k-party communication complexity, $C(g)$, of a function g in the minimum of costs of those k-party protocols which compute g.

As in the two-party case, every function can be computed by communicating $n+1$ bits. The theory of two-party communication games is well developed (cf. Lovász and Saks (1988) or Lovász (1989) for a survey), but much less is known about the multi-party communication complexity of functions. Babai *et al.* (1989) examined the *Generalized Inner Product* (GIP) function.

DEFINITION 1. Let $A \in \{0,1\}^{n\times k}$. We refer to the ith column of A as A_i, to the jth row of A as A^j, and to the ith entry in row j as A^j_i. Let GIP(A) denote the number of the all-1 rows of matrix A, modulo 2.

In other words, if column A_i is considered to be the characteristic vector of a subset Y_i of a fixed n-element set for $i=0, 1, ..., k-1$, then

$$\mathrm{GIP}(A) = |Y_0 \cap Y_1 \cap Y_2 \cap \cdots \cap Y_{k-1}| \mod 2.$$

In Babai *et al.* (1989), the following important lower bound is proved for the multi-party communication compexity of GIP:

THEOREM 2 (Babai *et al.*, 1989, Theorem 2).

$$C(\mathrm{GIP}) = \Omega\left(\frac{n}{4^k}\right). \quad \blacksquare$$

For the several interesting applications of Theorem 2 in Turing machine simulation tradeoffs or in circuit complexity theory, see (Babai *et al.*, 1989; Goldmann and Håstad, 1990). We describe a protocol, named "Telescope," in Section 2, which shows that the lower bound of Theorem 2 is close to the optimal:

THEOREM 3.

$$C(\mathrm{GIP}) \leqslant (2k-1)\left\lceil \frac{n}{2^{k-1}-1} \right\rceil.$$

Remarks. Independently from us, Nisan and Szegedy have also shown that the lower bound in Theorem 2 cannot be improved significantly (Babai, no date).

Babai *et al.* (1989) prove another $\Omega(n/c^k)$ lower bound for the k-party communication complexity of the *quadratic character* (Lengendre symbol)

of the mod p sum of k variables. They also mention that it would be important to find functions where the lower bound does not deteriorate exponentially as a function of k; e.g., a lower bound $\Omega(n/k^c)$ would be most desirable. Here we show that no such lower bound holds for the GIP function; but we do not know whether or not the other function of (Babai *et al.*, 1989) may satisfy such a stronger bound.

2. The Protocol

Consider an $n \times k$ binary matrix A with columns $A_0, A_1, A_2, ..., A_{k-1}$, where player P_i knows every column vector, except A_i, $i = 0, 1, 2, ..., k-1$.

We note that if it is known to P_0 that A has no row of the form $(0, 1, 1, ..., 1)$, then P_0 can simply announce the result by counting (mod 2) the number of rows of the form $(*, 1, 1, ..., 1)$. (All such rows must now begin with "1.")

The following lemma generalizes this idea:

Lemma 4. *Let $\alpha \in \{0, 1\}^k$. Suppose it is known to each player that α does not occur as a row of A. Then there exists a k-party protocol which computes* GIP(A) *with a communication of at most k bits.*

Proof. If α contains only 1's, GIP(A) = 0, and they are done, without communicating a bit.

Suppose now that α has some 0-coordinates. Without loss of generality we may assume that its first $l \geqslant 1$ coordinates are 0:

$$\alpha_0 = \alpha_1 = \cdots = \alpha_{l-1} = 0; \qquad \alpha_l = \alpha_{l+1} = \cdots = \alpha_{k-1} = 1.$$

Only the first k players, with corresponding 0 coordinates in α, will participate in the communication game. The game is played as follows:

Protocol Telescope. Let y_i denote the number of those rows of A of the form $(0, ..., 0, 1, ..., 1)$, where the first 1 occurs in position i.

For every i, $0 \leqslant i \leqslant l-1$, player P_i announces the parity of the number of rows of the form $(0, ..., 0, *, 1, ..., 1)$, where the $*$ is at place i.

Observation: This number is $y_i + y_{i+1}$.

Subsequently, each player privately computes the mod 2 sum of all numbers announced.

Observation: The result of this telescoping sum is $y_0 + y_l \bmod 2$. But, by assumption, $y_l = 0$; therefore the result is the desired quantity, $y_0 \bmod 2$.

The cost was l bits communication. ∎

Proof of Theorem 3. Let us divide the rows of matrix A into blocks of $2^{k-1} - 1$ contiguous rows plus a leftover of at most $2^{k-1} - 2$ rows. The

players cooperatively determine the number of all -2 rows in each block, and then privately add up the results to obtain GIP(A).

Next we show how to obtain the number of all -1 rows for a single block at the cost $2k-1$ bits of communication. P_0 knows all the columns, except the first, so he knows at most $2^{k-1}-1$ rows of length $k-1$, so he can find an $\alpha' \in \{0,1\}^{k-1}$, $\alpha' = (\alpha_1, \alpha_2, ..., \alpha_{k-1})$ which is not a row of the $k-1$ column wide part of the block seen by P_0. Let $\alpha = (0, \alpha_1, \alpha_2, ..., \alpha_{k-1})$. Then α does not occur as a row in this block. So if P_0 communicates α' with $k-1$ bits, then every player exchanges it to α privately, and they play the Telescope protocol with at most k bits, exchanging at most $2k-1$ bits in total. ∎

ACKNOWLEDGMENTS

The author thanks Laci Babai for many helpful comments and Gábor Tardos, whose remarks contributed significantly to the proof of Theorem 3.

RECEIVED July 12, 1991; FINAL MANUSCRIPT RECEIVED January 27, 1992

REFERENCES

BABAI, L., (no date), oral communication.

BABAI, L., NISAN, N., AND SZEGEDY, M. (1989), Multiparty protocols and pseudorandom sequences, *in* "Proceedings, 21st ACM STOC," pp. 1–11.

CHANDRA, A. K., FURST, M. L., AND LIPTON, R. J. (1983), Multi-party protocols, *in* "Proceedings, 15th ACM STOC," pp. 94–99.

GOLDMANN, M., AND HÅSTAD, J. (1990), On the power of small-depth treshold circuits, *in* "Proceedings, 31st IEEE FOCS," pp. 610–618.

LOVÁSZ, L. (1989), "Communication Complexity: A Survey," Technical Report CS-TR-204-89, Princeton University.

LOVÁSZ, L., AND SAKS, M. (1988), Lattices, Moebius functions and communication complexity, *in* "Proceedings, 29th IEEE FOCS," pp. 81–90.

YAO, A. C. (1979), Some complexity questions related to distributive computing, *in* "Proceedings, 11th ACM STOC," pp. 209–213.